Journal of Process Management and New Technologies
www.japmnt.com ISSN: 2334-735X (Print) ISSN: 2334-7449 (Online)
Vol. 10, Issue 3-4, 2022, pp. 75-92

CYBER SECURITY AND TOURISM: BIBLIOMETRIC ANALYSIS

Matija KOVAČIĆ[1*], Marko ČIČIN-ŠAIN[2], Vedran MILOJICA[3]

[1]*University North, Koprivnica, Croatia, matkovacic@unin.hr*
[2]*PAR University College Rijeka, Rijeka, Croatia, cicinsain.marko@gmail.com*
[3]*PAR University College Rijeka, Rijeka, Croatia, vedran.milojica@gmail.com*

Abstract: *The topic of cyber security in tourism is of particular importance since tourists in foreign countries are one of the most vulnerable groups due to a lack of knowledge of languages, laws, etc. With the increase in the number of technologies that enable interactivity, contactless payments, i.e., informative content for tourists, risks for the security of tourists' data as well as risks related to the theft of data on tourists' bank cards are emerging. In order to identify the current knowledge, i.e., the current situation in the context of research on cyber security in tourism, a bibliometric analysis was conducted, which indicated that an insufficient number of authors research cyber security and that there is not a sufficient number of studies that would analyze the mechanisms and measures of increasing cyber security in tourism. The importance of researching cyber security in tourism is based on the fact that tourism is a particularly vulnerable and sensitive branch of the economy to risks that affect tourists as such, and that it can depend on the reputation of the country, institutions, or hotels. The bibliometric analysis conducted in this paper is significant for future researchers considering that it can serve as a basis for researchers' focus on specific areas of cyber security.*

Keywords: *cyber security, tourism, risk, bibliometric analysis*

Original scientific paper
Received: 15.11.2022
Accepted: 02.12.2022
Available online: 08.12.2022

1. Introduction

The significance and importance of cyber security is growing with the growing importance of devices networking, which is stimulated by the development of Industry 4.0, i.e., the emergence of risks related to unauthorized access to information stored in databases as well as unauthorized taking over of control over the operation of machines and devices (Kim et al., 2021). The significance of cyber security is particularly pronounced in tourism, given that tourist destinations record a significant number of tourist visits, which means a significant number of risks related to the information security of tourists staying in hotels (Chen & Jai, 2019), the use of a large number of contactless payments with credit and debit cards on different points of sale (Cocosila & Trabelsi, 2016), QR codes that can lead to malicious content, which

[*] Corresponding author
Note: Paper is presented at the 8th international scientific conference „Innovation as the initiator of development“. Extended version of the paper is submitted to the Journal of Process Management and New Technologies.

can cause significant damage to the user who scans such a code (Krombholz et al., 2014), malware threats that can especially have a significant impact on tourists due to the possibility of being incorporated into different applications for smartphones (Apvrille, 2014), etc. All the described cyber security threats can cause significant damage to tourists, which can be related to downloading information about bank cards or bank accounts, downloading personal data of tourists, and the potential risk of selling them on the black market.

A particularly significant risk related to cyber security is booking accommodation through various internet services or mobile applications in which the user is required to enter data such as a bank card number. In practice, there are cases in which the aforementioned is used for bank transactions with stolen cards through fictitiously made bookings in fictitious accommodations, which is why organizations that provide booking services via mobile applications or websites hire specially trained staff who monitor such transactions and, if necessary, take measures to stop them, i.e., by revealing them, in order to protect users whose bank card data is exposed. Globally speaking, the problem of cyber security needs to be solved based on the risk analysis and the definition of preventive measures by which the identified risk will be reduced or completely eliminated. Only by proactive action, which includes education of tourists, education of service providers, implementation of physical mechanisms, and program protection mechanisms, can the risk of potential cyber threats be reduced (Li & Liu, 2021). Considering the importance that cyber security has in the context of the safety of tourists and the formation of the reputation of a safe tourist destination for visitors, the aim of this paper is to provide an overview of existing research in the field of cyber security in the context of tourist destinations and tourism in general.

The paper is based on a bibliometric analysis, which includes papers indexed in the WoS and Scopus databases and consists of five chapters. In the first chapter, the context and importance of Cyber Security in tourism is given, and potential threats in the context of Cyber Security are described. The second chapter provides an overview of existing research in the field of Cyber Security and the impact that Cyber Security has on tourism, i.e., tourist destinations. The methodology used is described in the third chapter, while the obtained results are described in the fourth chapter. The fifth chapter is the concluding chapter.

2. Overview of existing research

2.1. Cyber security

Cyber security can be conceptually defined as a set of mechanisms based on which an attempt is made to reduce the risk of unauthorized access or unauthorized use of data and information stored in database (Li & Liu, 2021), that is, in the context of cyber security related to devices, mechanisms that will prevent a possible takeover of control over physical devices (Williams & Woodward, 2015). In this context, the mechanisms represent the most common program barriers, such as firewalls and antivirus programs, as well as the implementation of penetration and other testing with the aim of identifying potential system weaknesses in order to eliminate them, and thereby eliminate the potential risk that may arise due to identified weaknesses (Min et al., 2015). In parallel with the development of cyber security strategies, there is also the development of new threats that aim to bypass cyber security mechanisms, which often include malicious software that is installed without the user's knowledge on the devices used by the user, monitors the user's use of the device, i.e., its search, and sends the collected information to the base. However, monitoring and documenting the user's behavior when using the device carries with it a significantly lower risk than the risk that occurs when installing software that can collect data from the user's bank account, that is, the user's official documents (Chiew et al., 2018).

Furthermore, the development of threats to cyber security is often associated with cyber terrorism, which is particularly significant if we are talking about cyber-attacks aimed at strategically important computer systems, or databases related to the normal functioning of the state. Cyber terrorism is often associated with attacks on the energy infrastructure as well as the financial infrastructure of the state, which creates not only the risk of taking personal data of users of financial institutions but also the risk of the normal development of social processes and security processes due to the threat of strategically important infrastructure (Plotnek & Slay, 2021).

When talking about cyber security, that is, information security, it is necessary to make a distinction. Cyber security refers to the security of digital data, i.e., computers and similar systems, while information security refers to the protection of business secrets, business documents, or in general, the protection of intellectual property (Von Solms & Van Niekerk, 2013). In other words, cyber security and information security can be intertwined if it is about information that has been digitized, which is why it is necessary to take care of the coordination of cyber security and information security management strategies (Sveen et al., 2009). In other words, the organizational system must have developed mechanisms to respond to information security challenges as well as cyber security challenges, which is achieved through the development of standard operating procedures, the implementation of norms, as well as the certification of management systems, which are directed towards the prevention of some of the most significant and frequent cyber threats (Hong, 2012). DDoS attacks (Distributed Denial of Service), which are most often directed towards the organization's Internet pages with the aim of congesting the pages and disabling them (Specht & Lee, 2003), i.e., the so-called Ransomware kit attacks that represent specially developed software packages that cause damage to the cyber system (Raunak & Krishnan, 2017). Thus, cyber security plays a particularly important role in the context of protecting user data as well as organizational data as a whole, the availability of which can result in the disclosure of business secrets or the theft of the user's identity, i.e., financial theft.

2.2. Cyber security in tourism

The tourism sector is one of the most vulnerable sectors when it comes to security and the impact that threats such as cyber terrorism have on it (Coca-Stefaniak & Morrison, 2018). The fundamental reason for this is the vulnerability of users of tourist services, especially because tourists represent people who are in most cases in other countries where they are not familiar with the customs and language, have a limited amount of financial resources to spend, and are therefore extremely vulnerable.

If we take a closer look at cyber security in tourism, it should be emphasized that with the development of technology comes the development of new technological innovations that enable increasing the interactivity of tourists with different content, i.e., carrying out different types of transactions in which tourists are asked to provide different personal data (Gretzel et al., 2015). In this context, various mobile applications are being developed that enable tourists to be informed about sights by scanning QR codes located next to the sights, etc. However, a more significant risk is identity theft using various phishing applications that can be incorporated into various tourist applications, and based on which can, among other things, steal the identity of tourists. Identity theft is particularly risky when talking about tourism, since tourists become aware of the theft after the theft has already occurred (Magliulo & Wright, 2014).

If we talk about cyber security and tourist facilities, i.e., primarily hotels, insufficiently protected hotel information systems can also be a source of risk for the identity of tourists as well as information on bank cards and similar, since in most cases tourists use credit or debit cards to pay for hotel services whose data, they leave on hotel websites that can be exposed to phishing applications (Rashid et al., 2020). In this context, the need to implement security certificates on the hotel's website comes to the fore, with the help of which the risk of theft is reduced but still remains present to a significantly lesser extent. Furthermore, considering that all hotel accommodations, as well as other tourist destinations, offer the possibility of using free Wi-Fi, there is a risk that the hotel Wi-Fi is used for attacks on smartphones or personal laptops of tourists, considering that in the hotel, each of guests can use Wi-Fi, which opens the possibility for malicious users to use this possibility for the purpose of theft (Lugovic et al., 2019).

The development of measures to reduce the risk of cyber-attacks, i.e., measures to increase cyber security in tourism, is particularly important for countries where tourism is the dominant branch, and an insufficient level of security can very quickly create a country's reputation as insecure, which will result in a potential risk in the long term for new tourist arrivals (Yang & Nair, 2014). The same applies to institutions, that is, to hotel accommodation, which is why it is especially important to pay attention to the education of hotel staff and investment in cyber risk reduction mechanisms in places where a large number of tourists are at the same time.

3. Methodology

The research is based on a bibliometric analysis of papers indexed in the WoS and Scopus databases according to the keywords "Cyber security" and "Tourism". The programming language R was used to carry out the bibliometric analysis. A similar methodology was used in scientific papers such as Kovačić et al. (2022), and Čiković et al. (2022). The research methodology is shown in Figure 1.

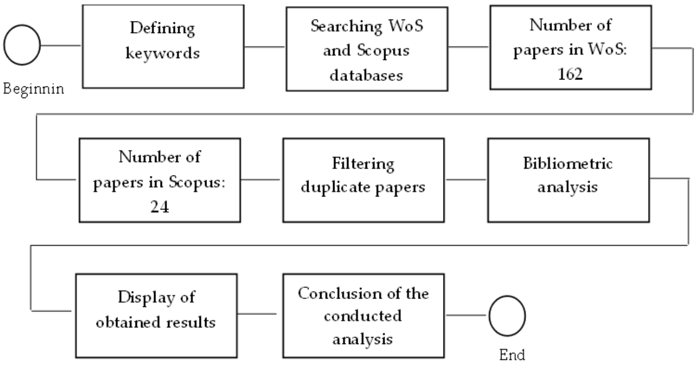

Beginnin
Defining keywords
Searching WoS and Scopus databases
Number of papers in WoS: 162
Number of papers in Scopus: 24
Filtering duplicate papers
Bibliometric analysis
Display of obtained results
Conclusion of the conducted analysis
End

Figure 1. Research methodology
Source: Authors´ analysis

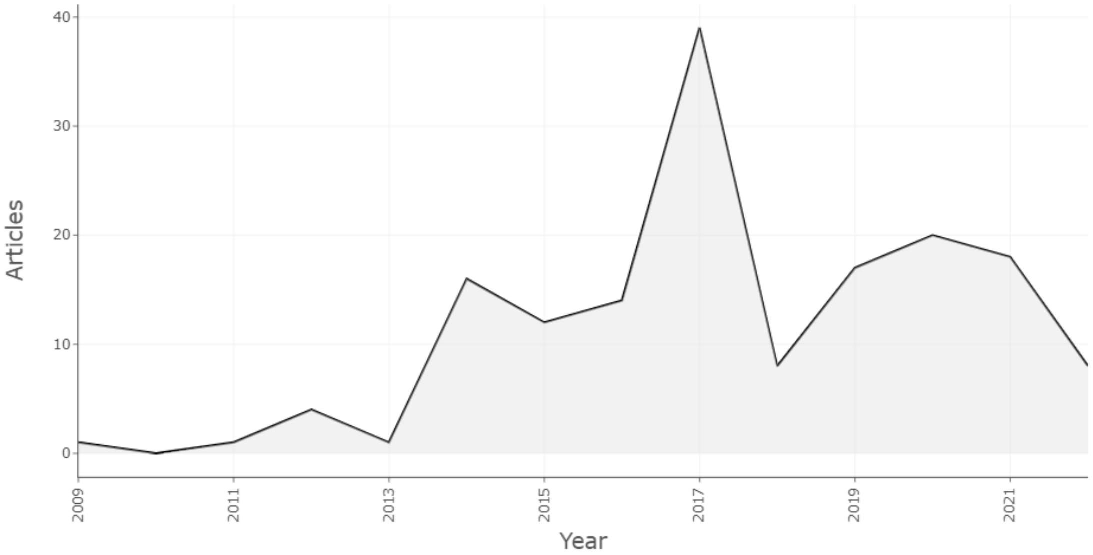
As shown in Figure 1, the search results in the WoS database generated a total of 162 results, while the search using the same keywords in the Scopus database generated a total of 24 results. All papers from 2009 to 2022 are included in the search. The results in both databases were combined and filtered in order to exclude papers that are identical from the research, after which a bibliometric analysis was performed based on the parameters of the average number of published papers, the average number of citations of published papers, the productivity of authors, the productivity of institutions, and journals in which the largest publication was published, the number of papers, and the most significant contribution of the papers in terms of the number of citations. All obtained research results are presented graphically and tabularly, and a conclusion is defined based on the obtained research results.

4. Research results

4.1. Cyber security in tourism

Graph 1 shows the analysis of the number of published papers in the period from 2009 to 2022. It is evident that there was a significant increase in the interest of researchers during 2017 related to the production of papers in the observed field. After 2017, the interest of researchers decreased, but the trend of stagnation remained. On the other hand, it should also be emphasized that until 2013, the interest of researchers in the observed area was small, which can be explained by the still insufficiently developed awareness and technology of Industry 4.0, which was in its infancy during that period.

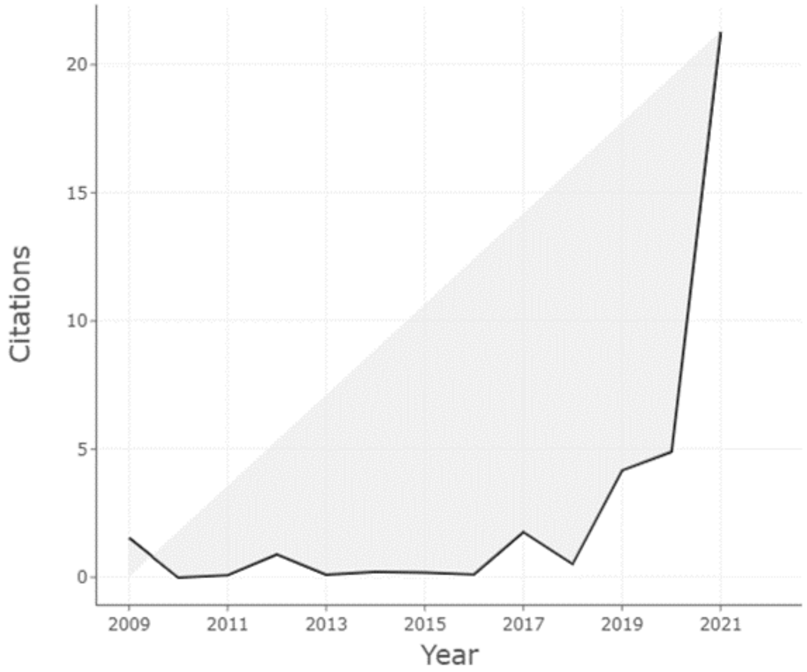
Globally speaking, the total number of authors who researched the impact of cyber security in tourism in the observed period is 497, of which 21 authors published their paper independently. On average, there are 3.4 authors per published paper. The average age of papers is 4.43 years, the average number of citations of papers is 7,864, i.e., the average growth of interest of researchers in the observed area is 17%.



Graph 1. Presentation of the average number of published papers in the period from 2009 to 2022

Source: Authors´ analysis

Graph 2 shows the average number of citations of published paper, which shows that the number of citations is growing and that a particularly significant increase in the number of citations was recorded in 2021, while in the period from 2009 to 2020, the number of citations stagnated or recorded a milder increase. This also indicates the increase in the attractiveness and significance of the analysis of cyber security in tourism. The results of the total number of citations for the year 2022 were not available at the time of writing the paper.



Graph 2. Analysis of the average number of citations in the period from 2009 to 2022.

Source: Authors´ analysis

4.2. Author's analysis

Table 1 shows the analysis of author productivity. Jinsu Kim (Jeju National University) stands out as the author with the largest number of articles in the observed field, while the other authors are equally represented with an equal number of papers. It should be emphasized that authors who have the same number of papers have equal importance in the table, regardless of their position.

Table 1. Analysis of author productivity

Authors	Affiliation	Articles
Jinsu Kim	Jeju National University	5
Jinde Cao	Southeast University	3
Jyh-An Lee	The Chinese University of Hong Kong	3
Mahasweta Sarkar	San Diego State University	3
Eun-Jun Yoon	Kyungil University	3

Source: Authors´ analysis

If the obtained results of the analysis of productivity of institutions and productivity of authors are compared, it is evident that there is a link since Jinde Cao is an author who is associated with Southeast University as the institution with the largest number of produced papers. It is necessary to emphasize that the number of papers by institutions includes all papers in the field of Cyber security in addition to paper that connect Cyber security with tourism.

4.3. Analysis of Institutions

Table 2 shows the productivity of institutions and the country from which the institution comes. The data shows that the institution with the largest number of papers from the observed area is Southeast University (13 papers), followed by the Electronics and Telecommunications

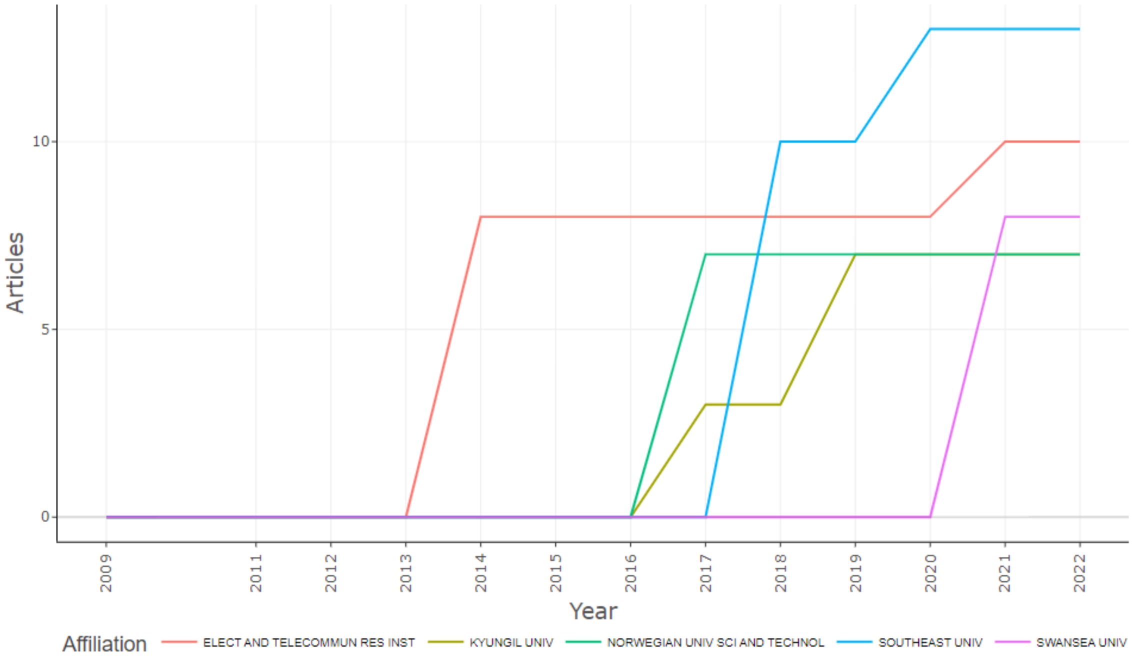
Research Institute (10 papers) and Swansea University (8 papers). Gyeongil University and Norwegian University of Science and Technology have an equal number of papers (7 papers) and their position in Table 2 has equal importance.

Table 2. Analysis of productivity of institutions

Affiliation	Country	Articles
Southeast University	Bangladesh	13
Electronics and Telecommunications Research Institute	South Korea	10
Swansea University	England	8
Gyeongil University	South Korea	7
Norwegian University of Science and Technology	Norway	7

Source: Authors´ analysis

The analysis of institutions can also be shown graphically using Graph 4, which shows the productivity of institutions visible in Table 2. Graph 4 also shows the production of papers per year, from which it can be concluded that all institutions record a trend of increasing the number of papers in the period from 2016-2022, for which the latest data is available. This can be interpreted as the need to consider the importance of Industry 4.0 as well as Cybersecurity due to the increasing potential in the application of technological innovations of Industry 4.0 as well as their spread in tourism.



Graph 4. Analysis of the productivity of institutions from 2009 to 2022

Source: Authors´ analysis

If we look at the productivity of the institutions, the Norwegian University of Science and Technology records the highest growth of produced papers since, according to the data obtained and shown on Graph 4, the mentioned institution had no published papers until 2017, but during 2017 there was a sudden increase in interest in observed area, and accordingly a sharp increase in the number of published papers.

4.4. Journal analysis

Table 3 shows the analysis of the number of papers published in journals. As visible from the table, the largest number of papers in the field of cyber security and its impact on tourism were published at conferences whose proceedings are indexed in the WoS and Scopus databases. It is necessary to draw attention to the fact that, as part of the conducted analysis, there are no journals in which the authors have the possibility of publishing their papers, but they send them exclusively to thematic conferences. The most important conference is MYCRIPT 2016 (30 published papers), followed by CRITIS 2014 with a total of 9 published papers.

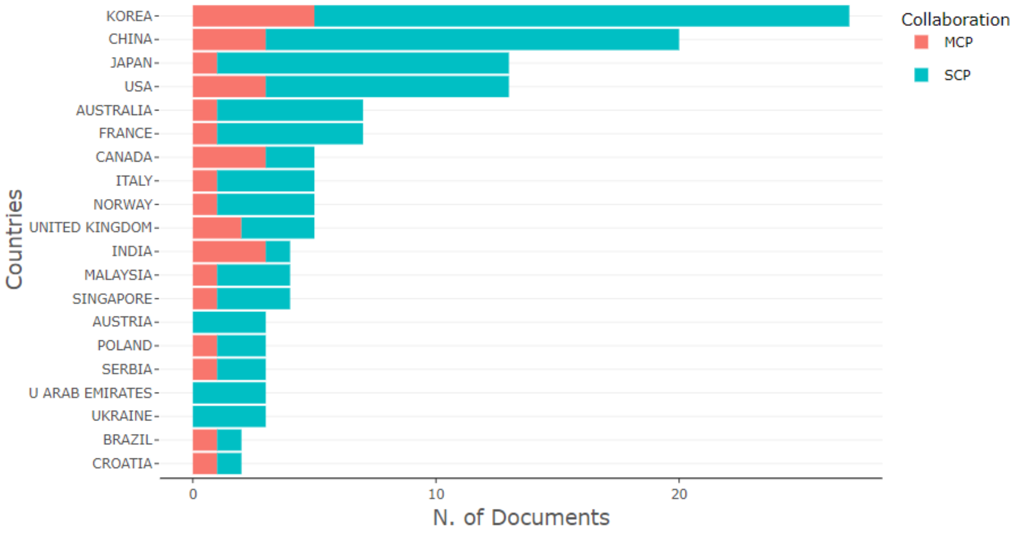
Table 3. Analysis of the most important journals and conference proceedings in the field of Cyber security in tourism

Sources	Articles
Paradigms in cryptology - MYCRIPT 2016: malicious and exploratory cryptology	30
Critical information infrastructures security (CRITIS 2014)	9
2014 IEEEE international conference (ITHINGS) - 2014 IEEEE international conference on green computing and communications (GREENCOM) - 2014 IEEEE international conference on cyber-physical-social computing (CPS)	7
2014 International conference on information and communication technology convergence (ICTC)	6
12th International conference on ICT convergence (ICTC 2021): beyond the pandemic era with ICT convergence innovation	5

Source: Authors´ analysis

4.5. Analysis of the productivity of countries

Chart 5 shows the analysis of the countries' productivity. It is evident that the country with the largest number of produced papers is South Korea, followed by China, Japan, and the USA in third place. Australia and France are in fourth place in terms of country productivity. If we compare the productivity of the countries shown on Chart 5 and technological progress, it is evident that the countries that are technologically most influential, that is, that have a developed IT industry, are ahead in looking at Cybersecurity compared to other countries that are less technologically developed.



Graph 5. Analysis of the productivity of countries from 2009 to 2022.

Source: Authors´ analysis

The productivity of the countries shown on Figure 2 can be graphically represented by Figure 2, where the number of published papers is shown in color. The greater the number of works produced by the country, the darker the shade of blue and vice versa. It should be emphasized that the countries marked in gray do not have a single paper recorded in the observed area, that is, at the time of the systematic analysis, not a single paper was published.

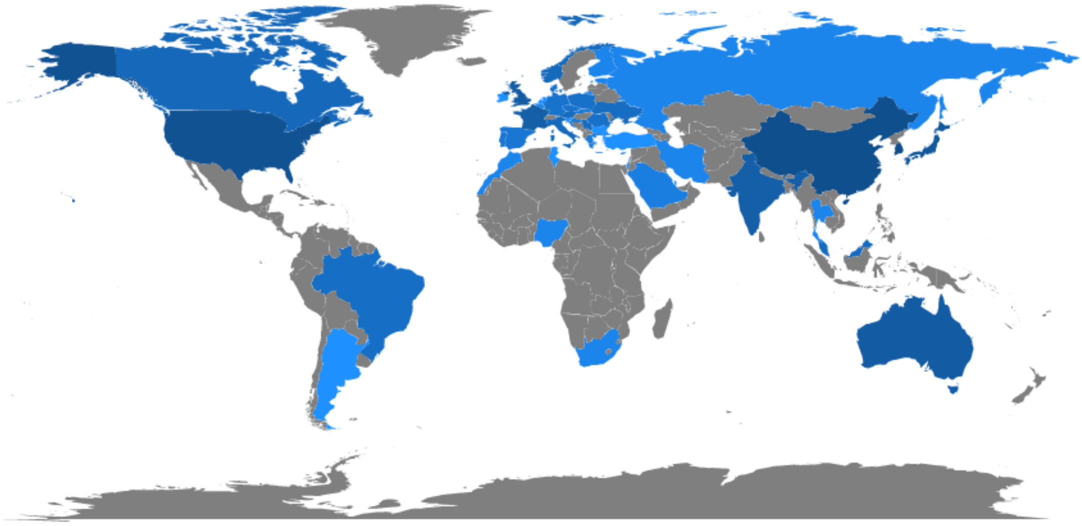


Figure 2. Overview of countries' productivity from 2009 to 2022.

Source: Authors´ analysis

4.6. Analysis of papers

Table 4 describes papers that, in terms of their significance and scientific contribution, have a particularly significant impact on the development of cyber security in tourism. As can be seen from the table, the largest number of papers are review papers that talk about the advantages of using technologies such as IoT, i.e., artificial intelligence. However, from the given overview, it is evident that the papers that are the most significant do not speak, i.e., do not investigate the direct impact that the threat of cyber security would have on tourists, which indicates that an insufficient number of authors deal with the field of cyber security in tourism.

Table 4. Analysis of the papers

Reference	Type of paper	Description of the research
Dwivedi et al. (2021)	Review paper	In the paper, the authors describe the emergence of new technologies as well as the importance of new technologies in the functioning of society. Among other things, the authors define the need for cyber security research and emphasize its importance when using technologies such as artificial intelligence, technologies used in healthcare, i.e., healthcare processes, technologies characteristic of financial institutions and similar.
Challa et al. (2017	Article	The authors focus on the challenges associated with the use of IoT and the advantages and disadvantages that come with it. They emphasize that the fundamental advantages relate to the possibility of creating interaction between several different devices and the possibility of automating the system, which is especially useful when talking about increasing the efficiency and

		effectiveness of a system such as a hotel system. However, on the other hand, they also emphasize the risks related to the possibility of third parties taking control of the IoT system, which can result in the risk of system collapse or malicious influence on IoT users.
Bodkhe et al. (2020)	Review paper	In looking at the possibility of increasing the security of the system, i.e., the resistance of the system against cyber-attacks, the authors talk about blockchain technology, which involves storing information in several different places, i.e., confirming requests for access to information stored, for example, in databases by several different nodes that are involved in blockchain. This alone reduces the risk of a third party being able to gain unauthorized access to information, which also means an increase in the reliability of the system from the point of view of cyber security.
Magliulo (2016)	Review paper	In the research, the author focuses on an overview of all the risks that can be identified in tourist destinations. The author defines identity theft as well as unauthorized access to tourist information as the most significant risks, which most often results in the construction of the tourist's identity. In order to reduce the aforementioned risk, the paper proposes a systematic approach to risk analysis and the definition of systematic risk reduction measures, since a partial approach often means the possibility that not all risks are addressed with preventive measures, which will not reduce the danger for the user, i.e., tourists.
Liao (2019)	Review paper	The research is based on the analysis and definition of the potential of VRGIS (Geographic Information System based on Virtual Reality) in the creation of a SMART tourist system that combines the possibility of displaying information about the tourist destination as well as user interaction with the system, i.e., options such as buying souvenirs, sending postcards to e-mail addresses, etc. In this context, the author emphasizes the crucial importance of ensuring a satisfactory level of cyber security in order to reduce the potential risk for users of such services.
Anichiti et al. (2021)	Case Study	In the article, the authors analyze hotel security in Romania and emphasize the need to ensure mechanisms that will create a safe environment for both the physical security of tourists and the information security of tourists. In this context, the authors reaffirm the importance of risk reduction through primary identification and then define measures aimed at risk mitigation. Furthermore, the authors emphasize the need for employee education so that employees can adequately and timely respond to security challenges.
Zaini et al. (2015)	Research Article	Research that analyzes the impact of security protocols, i.e., standard operating procedures that are activated in the event of a cyber-threat and organizational agility, The authors come to the realization that the crucial variable that can influence the organization's quick response to a threat is precisely the development of business continuity plans, based on which the threat response plan is also defined. In other words, the authors

		emphasize that the organization must be agile, which means that it must quickly and efficiently adapt and respond to identified risks, which is especially significant when talking about tourism.
Slapničar et al. (2022)	Review paper	The authors describe the procedure for conducting an internal audit related to cyber security and emphasize that the first step when defining the necessary improvements related to the current level of cyber security is the analysis of the existing situation, based on which potential vulnerabilities can be identified and, in accordance with the potential vulnerability of the system, the mechanism that will be defined to eliminate the identified vulnerability. Conducting an internal audit is also one of the fundamental steps when establishing an information security management system that can address some of the cyber security risks.
Kim et al. (2013)	Review paper	The authors investigate the impact of security, i.e., the reliability of the hotel's information system, on the reliability of the hotel system as a whole. In this context, the authors analyze potential threats to the information system, which could result in access to data located in the hotel's database, which is related to hotel service users. On the other hand, the authors also analyze the possibility of taking control over certain functions of the hotel system through the information system, which can also threaten both the security of the hotel and the security of the users in the hotel.
Chen & Jai, (2019)	Review paper	In the research, the authors analyze how the leakage of information from different sources in the hotel system affects the security of users; that is, the perception that users have regarding hotel accommodation. In this context, the authors come to the realization that it is necessary to develop crisis response plans through crisis management and procedures related to crisis management, for which it is necessary to ensure the competence of employees.

Source: Authors´ research

The topic of the impact of cyber risk, i.e., the insufficient level of cyber security on tourism, is evidently underrepresented. Generally speaking, the other papers included in the bibliometric analysis indicated that there is a significant number of papers that look at cyber security only in the context of production processes, that is, in the context of database security without a significant interdisciplinary approach, which is a significant problem. The reason for this is the growing number of different technological innovations that, on the one hand, allow increasing the satisfaction of users of tourist services while also opening up a significant space for potential cyber-attacks that can threaten the security of tourists and their confidential information.

4.7. Keyword analysis

Figure 3 shows the most frequently used keywords AND their link. It is evident from Figure 3 that the key words most often used in the analyzed papers are "Security"; "Attacks" and "Block ciphers" which are placed in the red cluster. In the blue cluster, the most frequently used keywords are "Management", "Things", "Challenges" and "Internet".

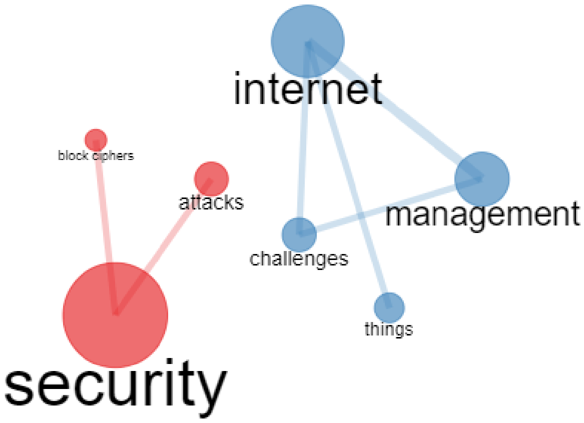


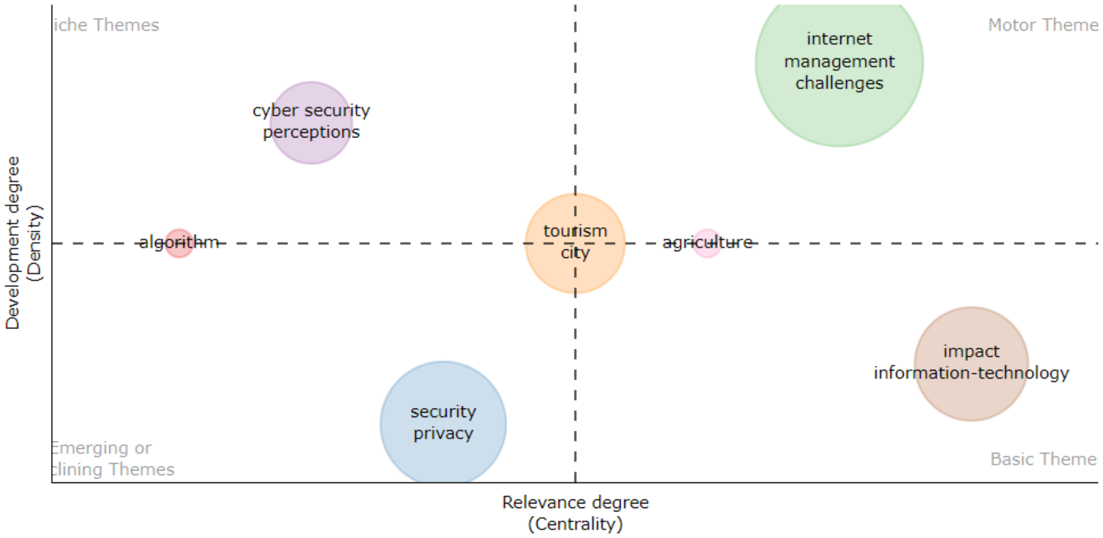
Figure 3. Keyword analysis.

Source: Authors´ analysis

It is necessary to draw attention to the fact that the clusters are not connected to each other, which can be a significant problem since cybersecurity is not viewed in the context of its management but exclusively through the context of cybersecurity as such and the variables that can affect its violation. However, on the other hand, it should be emphasized that the link between the keywords "management" and "Internet" indicates that the authors are increasingly analyzing the possibility of using the Internet and the potential that the Internet offers when managing the system, which can significantly affect the appearance of risks associated with system threats due to cyberattacks.

Furthermore, if we look at the evolution of the topics that the authors write about, Graph 6 shows that the focus of all authors' interests is tourism and cities, and that the topic that is the driving force behind the research is topics related to the use of the Internet in management and related challenges. Likewise, it is evident that topics that will become increasingly important in the future are related to security and privacy.

Based on the analysis of the evolution of the topics that the authors write about, it is evident that there is an interest among scientists in the field of security, and that a large number of scientists believe that the topic of tourism and the role that tourism plays in the development of cities is at the center of researchers' interests. On the other hand, the emergence of interests in the field of security and privacy will inevitably result in the conduct of new research in the future, which will aim to better understand the mechanisms by which the security of tourists will be increased. The obtained results indicate that the topic of cybersecurity is not yet sufficiently developed and that there is significant room for development since the importance of cybersecurity was recognized only at the beginning of 2016, according to the results obtained and presented on Graph 6.



Graph 6. Theme analysis.

Source: Authors´ analysis

4.8 Co-citation analysis

Figure 4 shows the co-citation analysis from which the influence of individual authors on other authors is visible. All authors are divided into clusters, the size of the circles shows the number of citations, the larger the circle, the greater the number of citations of the paper and vice versa. All circles are interconnected, and the thicker the line connecting the circles, the more significant the mutual cooperation, i.e. the influence of one research on another and vice versa. As an especially significant author, Bellare et. Al. (2016), who is also the main representative of the green cluster, and who in his research analyzes the impact that public video surveillance has on the safety of individuals in the city, that is, on their privacy. It is particularly interesting that within the green cluster Bellare et. Al. (2016) is also the only author since he mentions and builds on his previous research that was carried out in the past. It should also be emphasized that the green cluster is not connected to any other cluster. Furthermore, if we are talking about the blue cluster, the author who is the most significant is Kundsen L. who, in co-authorship with Wagner D., in the article "Integral Cryptanalysis" analyzes how certain cryptography methods are resistant to cyber attacks, that is, which of the cryptography methods is optimal in order to reduced the risk of a third party gaining access to sensitive data stored in databases (Kundsen and Wagner, 2022). The mentioned authors are also the most significant authors who have an influence on the other authors in the blue cluster.

The other clusters do not stand out in terms of their significance, which indicates a lack of understanding of the need to analyze the role that Cybersecurity plays in tourism. It is particularly important to emphasize that none of the clusters are interconnected, which means that there is no significant collaboration between the authors. A lack of cooperation can also mean a lack of knowledge transfer and follow-up on other research conducted by other authors. In the same way, it is necessary to draw attention to the age of the references cited in the clusters, since some references, such as the example in the blue cluster, are older than 25 years, which indicates that research that is outdated in its significance is being used.

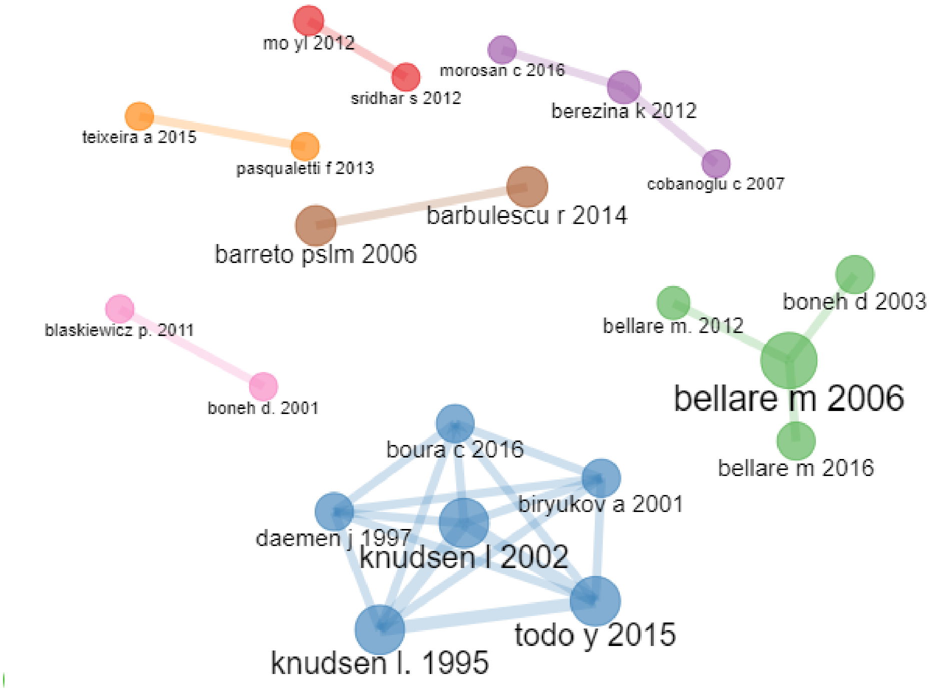


Figure 4. Co-citation analysis.

Source: Authors´ analysis

4.9 GAP Analysis

Based on the conducted analysis, it was identified that an insufficient number of authors consider the impact that cyber security has on tourism, that is, the security of tourists' personal information. Likewise, it was identified that the authors do not cooperate on joint research, which can also be a significant problem, since without knowledge sharing and mutual cooperation there is a risk of partial consideration of the issue of cybersecurity in tourism. It is particularly important to emphasize that during the research, a lack of papers was identified that would analyze the security of information systems within the hotel, which can result in the risk of a third party taking over information or part of the information about tourists who are currently staying in the hotel.

There is no doubt that the topic of cybersecurity analysis is new, and its importance is growing with the growth of technological innovations and the use of the Internet. However, considering that tourism is a particularly sensitive branch to threats, i.e. security, there is no doubt that there is a need for a more detailed review of the mechanisms by which the existing level of cyber security of tourists would be increased, as well as the protection mechanisms of information systems as well as the technological solutions used in general in tourism.

One of the biggest GAPs that was identified during the research are empirical type studies that analyze the current situation in the context of cybersecurity in the hotel industry. The majority of authors focus on the literature review without looking at the current situation and existing issues of cybersecurity in the tourism sector, which may mean the risk that the development of new models for increasing cybersecurity will not be based on real problems and real threats, but on conceptual models that are theoretical in nature, and therefore questionable applicability. In view of this, it is necessary to start with an inductive approach, which involves analyzing problems and defining solutions for identified problems based on scientific and other research.

4.10 Discussion

There is no doubt that tourism is a particularly sensitive branch, especially due to the fact that it is based on reputation, which can be easily damaged due to poor service, insufficient security of tourists, etc. (Artigas et al., 2015). Furthermore, given that tourism is a particularly important branch for the Mediterranean countries, where it has a significant share of the total GDP, countries must be aware of the importance of developing tourist protection mechanisms, which is especially significant due to the increasing importance and imperative of implementing technologies that are based on mutual communication and data collection. An insufficient level of security for the collected data may consequently result in a risk for tourists whose data is collected and stored in such databases (Paraskevas, 2022). Furthermore, considering that the imperative to use online booking is increasingly being placed, and this is especially important for tourists coming from different countries, it is necessary to take care of the security of the online booking service, since an insufficient level of security can result in the appearance of risks for the data that tourists leave on such services, that is, for the data saved in the online booking service databases (Fragniere and Yagci, 2021).

However, with the development of technology and the emergence of Industry 4.0, which is based on automation and mutual communication between different technologies as well as enhancing the application of technologies such as virtual reality and similar (Buntak et al., 2021), the mentioned can affect the attractiveness of the tourist destination and thus the satisfaction of tourists who visit tourist destinations that offer virtual content. In cases where tourists are required to provide credit or debit card information in order to use such systems, there is a significant risk that the information provided will be available to third parties that are often unwelcome, which may result in harm to tourists.

It was precisely the use of contactless payment, as well as bank transactions via the Internet in general, that became particularly important during the coronavirus pandemic, where the non-cash payment method was emphasized, which made it imperative to provide additional protection of the channels through which tourists used to make transactions, as well as to generally increase the security of such transactions (Emms et al., 2013). However, despite this, through the research, it was identified that an insufficient number of authors perceive and research the importance of ensuring cyber security in tourist destinations, which can be an opportunity for new researchers who are just starting to research this area, but on the other hand, it can also represent a significant problem, since the lack of research can also mean the impossibility of practitioners creating protection mechanisms.

Undoubtedly, one of the technologies that can be used to increase payment security and generally reduce the risk of cyber-attacks is the blockchain, which stores data in several different locations and thus reduces the risk of data being accessible to third parties. The application of blockchain technology is especially important when talking about payments since it can be used to verify payments, given that several different nodes in the blockchain network must confirm the transaction, i.e., they must verify it in order for it to be valid. Accordingly, there is no doubt that in the future blockchain technology will be used for the purpose of increasing the security of tourist destinations as well as tourist services, and that new technologies that are developing within Industry 4.0 will result in the emergence of new innovations that will further increase the possibility of personalizing tourist services and increasing the quality of service provided to users. This is supported by the development of so-called "SMART" tourism, which includes the aforementioned digitization and automation in the provision of tourist services.

Conclusion

In the conducted bibliometric analysis, it was identified that an insufficient number of authors deal with addressing cyber risks in the tourism sector, that is, tourism as such in general. This indicates an insufficiently developed awareness of the need to mitigate such risks, as well as an insufficiently developed awareness of the importance of tourist information security. Furthermore, with the development of applications that enable the booking of accommodation, that is, the booking of flights and other tourist services, there is also the possibility of misuse of such applications in the context of the development of malware and the development of patches that will enable the collection of data of people making bookings. This alone creates a significant risk that is connected to the security of tourists' financial resources or, in general, the security of official documents that tourists have and must use when booking.

As one of the technologies that can be highlighted as a technology that has significant potential in increasing cyber security, blockchain technology stands out, which as such is still in its infancy and only in the future is expected to use the full potential that blockchain has. In addition, the education of users of tourist services who use mobile and internet applications for booking and similar activities in the context of security and the data they can safely share is particularly important, since education and cyber literacy is one of the first steps towards increasing cyber security, and thereby protecting tourists.

This research has limitations related to the selection of search parameters, i.e., an exclusive focus on cyber security in tourism in general without a focus on individual tourism branches. With this in mind, future researchers in this area are recommended to conduct primary research with the aim of examining the current situation in tourist facilities in the context of preparedness for cyber security risks.

References

Anichiti, A., Dragolea, L.L., Tacu Hârșan, G.D., Haller, A.P. & Butnaru, G.I. (2021). Aspects regarding safety and security in hotels: Romanian experience. *Information*, 12(1), 1-22.

Apvrille, A. (2014). The evolution of mobile malware. Fraud & Security, 2014(8), 18-20.

Artigas, E. M., Vilches-Montero, S., & Yrigoyen, C. C. (2015). Antecedents of tourism destination reputation: The mediating role of familiarity. *Journal of Retailing and Consumer Services*, 26, 147-152.

Bellare, M., Fuchsbauer, G., & Scafuro, A. (2016). *NIZKs with an untrusted CRS: security in the face of parameter subversion*. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 777-804). Springer, Berlin, Heidelberg.

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for industry 4.0: A comprehensive review," *IEEE Access*, 79764-79800.

Buntak, K., Kovačić, M., & Mutavdžija, M. (2021). Application of Artificial Intelligence in the business. *International journal for quality research*, 15(2), 403-416.

Challa, S., Wazid, M., Das, A.K., Kumar, N., Reddy, A.G., Yoon, E.J., & Yoo, K.Y. (2017). Secure signature-based authenticated key establishment scheme for future IoT applications. *IEEE Access*, 3028-3043.

Chen, H.S. & Jai, T.M.C. (2019). Cyber alarm: Determining the impacts of hotel's data breach messages. *International Journal of Hospitality Management*, 82, 326-334.

Chiew, K.L., Yong, K.S.C. & Tan, C.L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, 106, 1-20.

Čiković, K.F., Martinčević, I. & Lozić, J. (2022). Application of Data Envelopment Analysis (DEA) in the Selection of Sustainable Suppliers: A Review and Bibliometric Analysis. *Sustainability*, 14(11), 1-30.

Coca-Stefaniak, A. & Morrison, A.M. (2018). City tourism destinations and terrorism–a worrying trend for now, but could it get worse?. *International Journal of Tourism Cities*, 4(4), 409-412.

Cocosila, M. & Trabelsi, H. (2016). An integrated value-risk investigation of contactless mobile payments adoption. *Electronic Commerce Research and Applications*, 20, 159-170.

Dwivedi, Y.K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., & Williams, M.D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 57, 101994.

Emms, M., Arief, B., Little, N., & Moorsel, A. V. (2013). *Risks of offline verify PIN on contactless cards*. In International Conference on Financial Cryptography and Data Security (pp. 313-321). Springer, Berlin, Heidelberg.

Fragniere, E., & Yagci, K. (2021). *Network & Cyber Security in Hospitality and Tourism*. University of South Florida M3 Center Publishing, 17(9781732127593), 7.

Gretzel, U., Sigala, M., Xiang, Z., & Koo, C. (2015). Smart tourism: foundations and developments. *Electronic markets*, 25(3), 179-188.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, 55(1), 74-81.

Kim, H.B., Lee, D.S., & Ham, S. (2013). Impact of hotel information security on system reliability. *International Journal of Hospitality Management*, 35, 369-379.

Kim, K., Kim, J. S., Jeong, S., Park J. H., & Kim, H.K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security*, 103, 102150.

Knudsen, L., & Wagner, D. (2002). *Integral cryptanalysis*. In International Workshop on Fast Software Encryption (pp. 112-127). Springer, Berlin, Heidelberg. 2002

Kovačić, M., Mutavdžija, M., & Buntak, K. (2022). New Paradigm of Sustainable Urban Mobility: Electric and Autonomous Vehicles—A Review and Bibliometric Analysis. *Sustainability*, 14(15), 1-23.

Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M. & Weippl, E. (2014). QR code security: A survey of attacks and challenges for usable security. International Conference on Human Aspects of Information Security, Privacy, and Trust, Heraklion, Crete, Greece, 79-90.

Li, Y. & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, 8176-8186.

Liao, Y. (2019). Research and implementation of the intelligent tourism system based on VRGIS. The International Conference on Cyber Security Intelligence and Analytics, Shenyang, China, 130-135.

Lugovic, S., Mrsic, L., & Korona, L.Z. (2919). Public WiFi security network protocol practices in tourist destination. 16th International Symposium on Pervasive Systems, Algorithms and Networks I-SPAN 2019, Naples, Italy, 321-332.

Magliulo, A. & Wright A.C. (2014). C*yber Security in Tourism: The Role of Awareness*. In: M. Sitek, I. Niedziótka, A. Ukleja (Eds.), Consumer Protection, (pp. 71-96). Alcide De Gasperi University Józefów.

Magliulo, A. (2016). Cyber security and tourism competitiveness. *European Journal of Tourism, Hospitality and Recreation*, 7(2), 128-134.

Min, K.S., Chai, S.W. & Han, M. (2015). An international comparative study on cyber security strategy. *International Journal of Security and its Applications*, 9(2), 13-20.

Paraskevas, A. (2022). *Cybersecurity in travel and tourism: a risk-based approach*. In Handbook of e-Tourism (pp. 1605-1628). Cham: Springer International Publishing.

Plotnek, J.J. & Slay, J. (2021). Cyber terrorism: A homogenized taxonomy and definition. *Computers & Security*, 102, 102145.

Rashid, J., Mahmood, T., Nisar, M.W. & Nazir, T. (2020). Phishing detection using machine learning technique. 2020 First International Conference of Smart Systems and Emerging Technologies (SMARTTECH), Riyadh, Saudi Arabia, 43-46.

Raunak, P. & Krishnan, P. (2017). Network detection of ransomware delivered by exploit kit. *ARPN Journal of Engineering and Applied Sciences*, 12(2), 3885-3889.

Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, 44, 1-22.

Specht, S. & Lee, R. (2003). *Taxonomies of distributed denial of service networks, attacks, tools and countermeasures*. CEL2003-03, Princeton University, 1-20.

Sveen, F.O., Torres, J.M. & Sarriegi, J.M. (2009). Blind information security strategy. *International Journal of Critical Infrastructure Protection*, 2(3), 95-109.

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & security*, 38, 97-102.

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical devices*, 8, 305–316.

Yang, E.C.L. & Nair, V. (2014). Tourism at risk: A review of risk and perceived risk in tourism. Asia-Pacific Journal of Innovation in Hospitality and Tourism (APJIHT), 3, 1-21.

Zaini, M.K., Masrek, M.N., & Abdullah Sani, M.K.J. (2015). A Conceptual Overview on the Relationship Between Information Security Practices and Organizational Agility. *Advanced Science Letters,* 21(5), 1289-1292.